AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter. [Use ~~strikethrough~~ for deleted matter (or double square brackets "[[]]" if the strikethrough is not easily perceivable, *i.e.*, "4" or a punctuation mark) and underlined for added matter.]

1. (Currently amended) A method of delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout station, the method comprising:

receiving and securely retaining a digital document and a transmitted independently verifiable data record of the intended recipient at a printout station, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender;

obtaining a second token relating to the first token of the sender;

obtaining a first token of the intended recipient;

decoding the encrypted digest using the second token of the sender;

using a hash algorithm to create a digest of the document; ~~and~~

comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient; and

releasing the document when the intended recipient has proved their identity by use of a second token that is uniquely related to the first token of the intended recipient.

2. (Original) A method according to Claim 1, wherein the receiving step comprises receiving a digital certificate of the sender.

3. (Currently amended) A method according to Claim 2, wherein the obtaining step comprises the second token of the sender being sent as part of the sender's digital certificate.

4. (Original) A method according to Claim 2, further comprising carrying out an on-line check of the validity of the sender's certificate.

5. (Currently amended) A method according to Claim 1, wherein the first and second tokens of the sender comprise private and public encryption/decryption keys of the sender.

6. (Original) A method according to Claim 1, further comprising printing out a copy of the document once the sender and the document have been authenticated.

7. (Original) A method according to Claim 6, wherein the method further comprises printing a verifying mark on the printed copy of the document to signify its authenticity.

8. (Original) A method according to Claim 1, wherein the transmitted document comprises a fax document.

9. (Currently amended) A method of sending and delivering a digital document to an intended recipient at a printout station together with data enabling the document and the sender to be authenticated, the method comprising:

creating a digest of the document using a hash algorithm;

obtaining a first token of the intended recipient;

encrypting the digest using a first token of the sender;

obtaining a second token relating to the first token of the sender, which can be used to decrypt the encrypted digest;

sending the encrypted digest, the digital document and the second token of the sender to the recipient;

receiving and securely retaining a transmitted document and a transmitted independently verifiable data record of the intended recipient at a printout station;

requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient; and

releasing the document when the intended recipient has proved their identity by use of a second token that is uniquely related to the first token of the recipient.

10. (Original) A method according to Claim 9, wherein the transmitted document is a fax document.

11. (Currently amended) A method according to Claim 9, further comprising the sender proving their identity prior to the sending step by transferring data from a personal portable data carrier holding the first token of the sender to a transmission station from which the document is to be sent.

12. (Original) A method according to Claim 11, wherein the proving step further comprises the sender entering a verifiable security identifier into the transmission station to establish that they are the legitimate owner of the portable data carrier.

13. (Original) A method according to Claim 11, wherein the step of encrypting the digest comprises supplying the digest of the document from the transmission station to the portable data carrier of the sender, encrypting the digest of the document on the portable data carrier, and returning the encrypted digest of the document from the portable data carrier to the transmission station.

14. (Currently amended) A method according to any of Claim 9, further comprising obtaining details of the sender including the second token of the sender prior to transmitting the document.

15. (Currently amended) A method according to Claim 14, wherein the step of obtaining details comprises obtaining the sender's details from a central database storing second tokens of the senders and other sender's details.

16. (Currently amended) A method according to Claim 14, wherein the sender's details and the second token of the sender are provided in a sender's digital certificate.

17. (Currently amended) A method according to any of Claim 9, wherein the first and second tokens of the sender comprise private and public encryption/decryption keys of the sender.

18. (Currently amended) A device for delivering and determining the authenticity of a digital document sent by an unknown sender to an intended recipient at a printout

station ~~determining the authenticity of a digital document sent by an unknown sender~~, the device comprising:

a communications module arranged to receive ~~the document~~ an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, an encrypted digest of the document created by the sender using a hash algorithm, the digest being encrypted using a first token of the sender, and a second token relating to the first token of the sender;

a store for securely retaining the transmitted document, the transmitted independently verifiable data record and the first token of the intended recipient;

an instruction module for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record; and

a controller arranged to decode the encrypted digest using the second token of the sender; creating a digest of the document using a hash algorithm; ~~and~~ comparing the decrypted received digest with the newly created digest to determine the authenticity of the sender and the document; and releasing the document when the intended recipient has proved their identity by use of a second token of the intended recipient that is uniquely related to the first token of the intended recipient.

19. (Currently amended) A device for sending and delivering a digital document to an intended recipient at a printout station together with data enabling the document and the sender to be authenticated ~~sending a digital document to a recipient together with data enabling the document and the sender to be authenticated~~, the device comprising:

a controller arranged to create a digest of the document using a hash algorithm and to encrypt the digest using a first token of the sender, and to release the document when the intended recipient has proved their identity by use of a second token of the intended recipient that is uniquely related to the first token of the intended recipient;

a store for securely retaining the transmitted document, the transmitted independently verifiable data record and the first token of the intended recipient;

an instruction module for requesting proof of the intended recipient's identity using data provided in the intended recipient's data record; and

a communications module arranged to obtain an electronic version of the transmitted document over a communications network, an independently verifiable data record of the intended recipient, a first token of the intended recipient, a second token of the sender related to the first token of the sender, which can be used to decrypt the encrypted digest and to send the encrypted digest, the digital document and the second token to the recipient.